COURSE SYLLABUS

Vulnerability Management for Federal Systems Course (Self-Paced)

Learn why federal agencies patch and scan the way they do, and how to report vulnerability posture in terms leaders can act on.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/vulnerability-management-for-federal-systems-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: Why Vulnerability Management Runs the Program

- Lessons:
  - The Cost of Unpatched Systems
  - From Vulnerability to Exploit: How Adversaries Operate
  - The Federal Vulnerability Management Mandate Landscape
  - Program Ownership: Roles from ISSO to CISO
- Applied activity: Learners walk through a case study timeline from vulnerability disclosure to exploitation to organizational impact, and identify the point where a faster patching decision would have changed the outcome.

Module 2: Asset Visibility and the CDM Program

- Lessons:
  - Why You Cannot Patch What You Cannot See
  - BOD 23-01: Asset Visibility and Vulnerability Detection Requirements
  - The Continuous Diagnostics and Mitigation Program
  - Building and Maintaining an Asset Inventory
- Applied activity: Given a sample asset list with known gaps, learners identify which systems are missing from inventory and what BOD 23-01 would require the agency to do next.

Module 3: The KEV Catalog and Exploitation-Based Prioritization

- Lessons:
  - Severity Scores Are Not Enough: The Limits of CVSS Alone
  - Inside the CISA Known Exploited Vulnerabilities Catalog
  - Building a Risk-Based Remediation Priority List
  - Case Walkthrough: Tracing a KEV Entry to a Remediation Deadline

- Applied activity: Given a short list of vulnerabilities with CVSS scores, learners cross-reference which ones appear on the KEV catalog and re-order the remediation priority list accordingly.

Module 4: BOD 26-04 Tiers and Remediation Timelines

- Lessons:
  - What a Binding Operational Directive Requires
  - BOD 26-04 Tiering Structure Explained
  - Remediation Timelines and Compliance Reporting
  - Common Compliance Gaps and How Programs Close Them
- Applied activity: Given a discovered vulnerability's characteristics, learners determine which BOD 26-04 tier it falls into and calculate the remediation deadline.

Module 5: Patch Management Planning per NIST SP 800-40

- Lessons:
  - The Enterprise Patch Management Lifecycle
  - Planning, Testing and Staging Patches
  - Patch Prioritization Strategies from SP 800-40
  - Handling Exceptions, Legacy Systems and Compensating Controls
- Applied activity: Learners draft a patch management plan outline for a hypothetical system, including testing and staging steps and one legacy-system exception.

Module 6: Vulnerability Scanning Programs and Scan Cadence

- Lessons:
  - Types of Vulnerability Scans and What Each One Reveals
  - Setting Scan Scope, Cadence and Credentials Policy
  - Reading a Scan Report Without Running One
  - Where Scanning Fits in the Larger Program
- Applied activity: Learners review a sample scan report excerpt and identify scan type, scope, and what follow-up action the findings require, without running a scanner.

Module 7: Reporting Vulnerability Posture to Leadership

- Lessons:
  - Metrics That Matter to Executives
  - Building a POA&M and Tracking Remediation
  - Communicating Risk Without Jargon
  - Briefing Leadership: A Model Vulnerability Posture Report
- Applied activity: Learners convert a set of technical scan and remediation results into a two-paragraph leadership brief and a one-page POA&M excerpt.